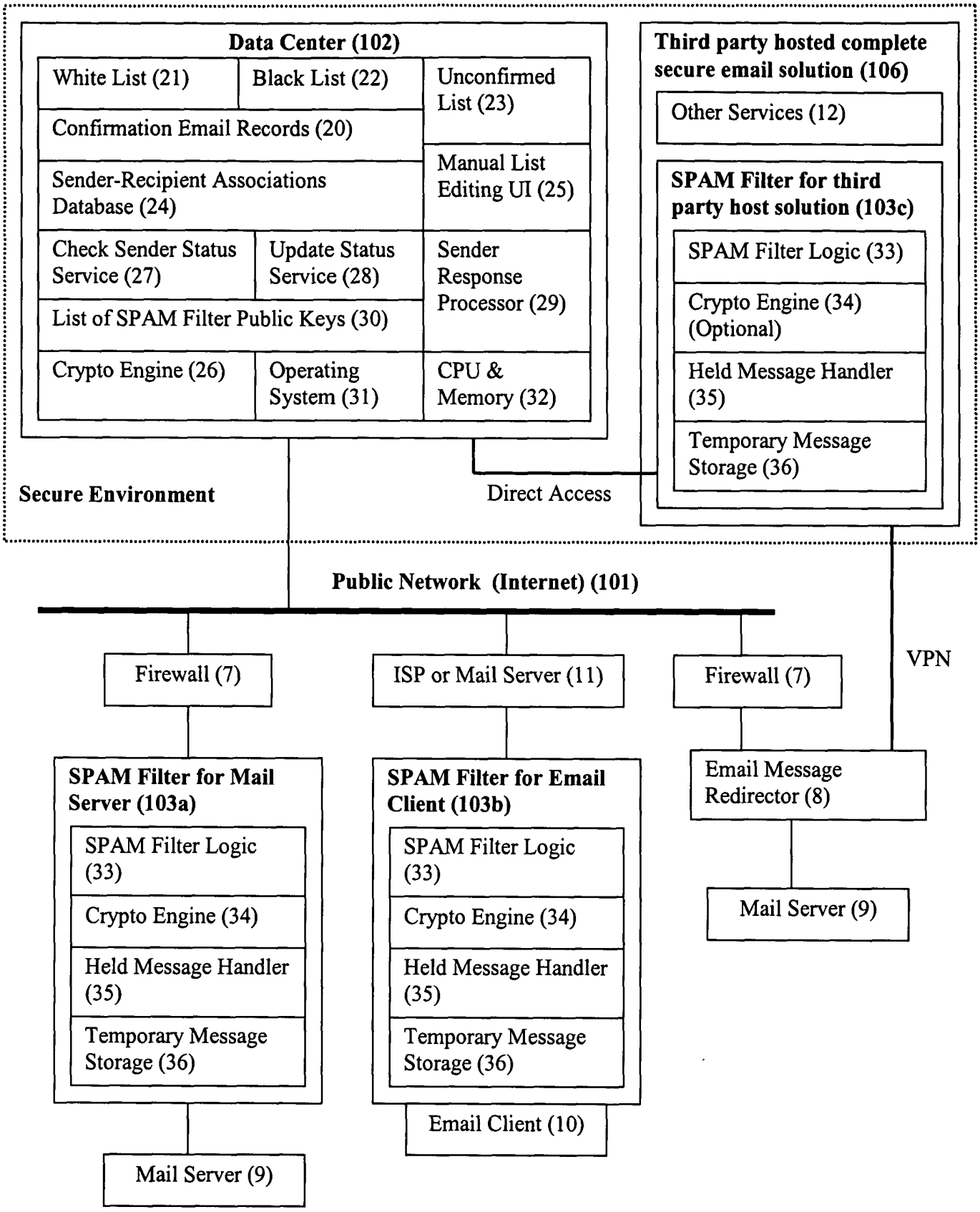
Data Center (102)
White List (21)
Black List (22)
Unconfirmed List (23)
Confirmation Email Records (20)
Manual List Editing UI (25)
Sender-Recipient Associations Database (24)
Check Sender Status Service (27)
Update Status Service (28)
Sender Response Processor (29)
List of SPAM Filter Public Keys (30)
Crypto Engine (26)
Operating System (31)
CPU & Memory (32)
Third party hosted complete secure email solution (106)
Other Services (12)
SPAM Filter for third party host solution (103c)
SPAM Filter Logic (33)
Crypto Engine (34) (Optional)
Held Message Handler (35)
Temporary Message Storage (36)
Secure Environment
Direct Access
Public Network (Internet) (101)
VPN
Firewall (7)
ISP or Mail Server (11)
Firewall (7)
SPAM Filter for Mail Server (103a)
SPAM Filter Logic (33)
Crypto Engine (34)
Held Message Handler (35)
Temporary Message Storage (36)
SPAM Filter for Email Client (103b)
SPAM Filter Logic (33)
Crypto Engine (34)
Held Message Handler (35)
Temporary Message Storage (36)
Email Message Redirector (8)
Mail Server (9)
Email Client (10)
Mail Server (9)

Figure 1.

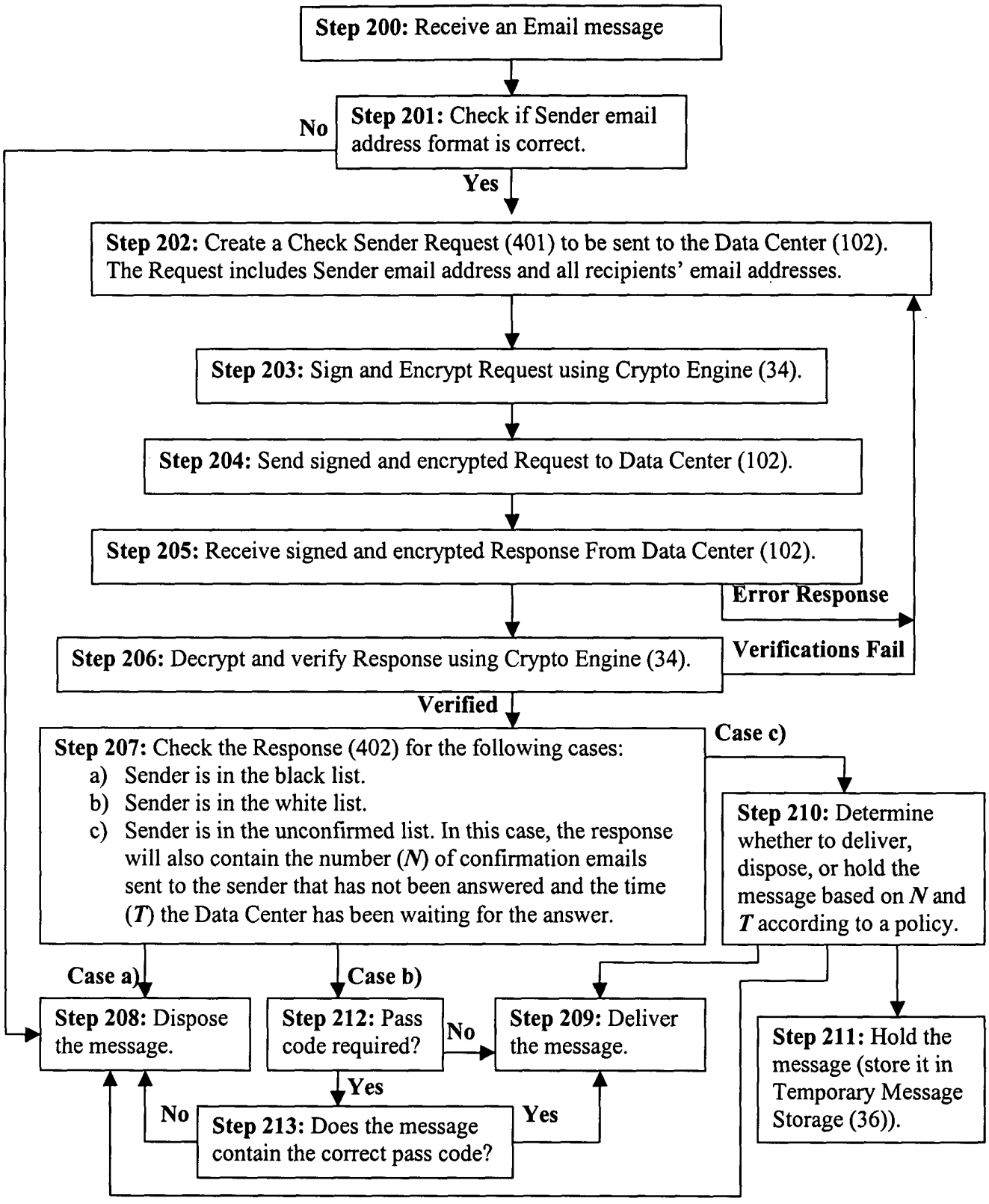
Step 200: Receive an Email message
Step 201: Check if Sender email address format is correct.
No
Yes
Step 202: Create a Check Sender Request (401) to be sent to the Data Center (102). The Request includes Sender email address and all recipients' email addresses.
Step 203: Sign and Encrypt Request using Crypto Engine (34).
Step 204: Send signed and encrypted Request to Data Center (102).
Step 205: Receive signed and encrypted Response From Data Center (102).
Error Response
Step 206: Decrypt and verify Response using Crypto Engine (34).
Verifications Fail
Verified
Step 207: Check the Response (402) for the following cases:
a) Sender is in the black list.
b) Sender is in the white list.
c) Sender is in the unconfirmed list. In this case, the response will also contain the number (N) of confirmation emails sent to the sender that has not been answered and the time (T) the Data Center has been waiting for the answer.
Case c)
Step 210: Determine whether to deliver, dispose, or hold the message based on N and T according to a policy.
Case a)
Case b)
Step 208: Dispose the message.
Step 212: Pass code required?
No
Step 209: Deliver the message.
Step 211: Hold the message (store it in Temporary Message Storage (36)).
Yes
No
Step 213: Does the message contain the correct pass code?
Yes

Figure 2

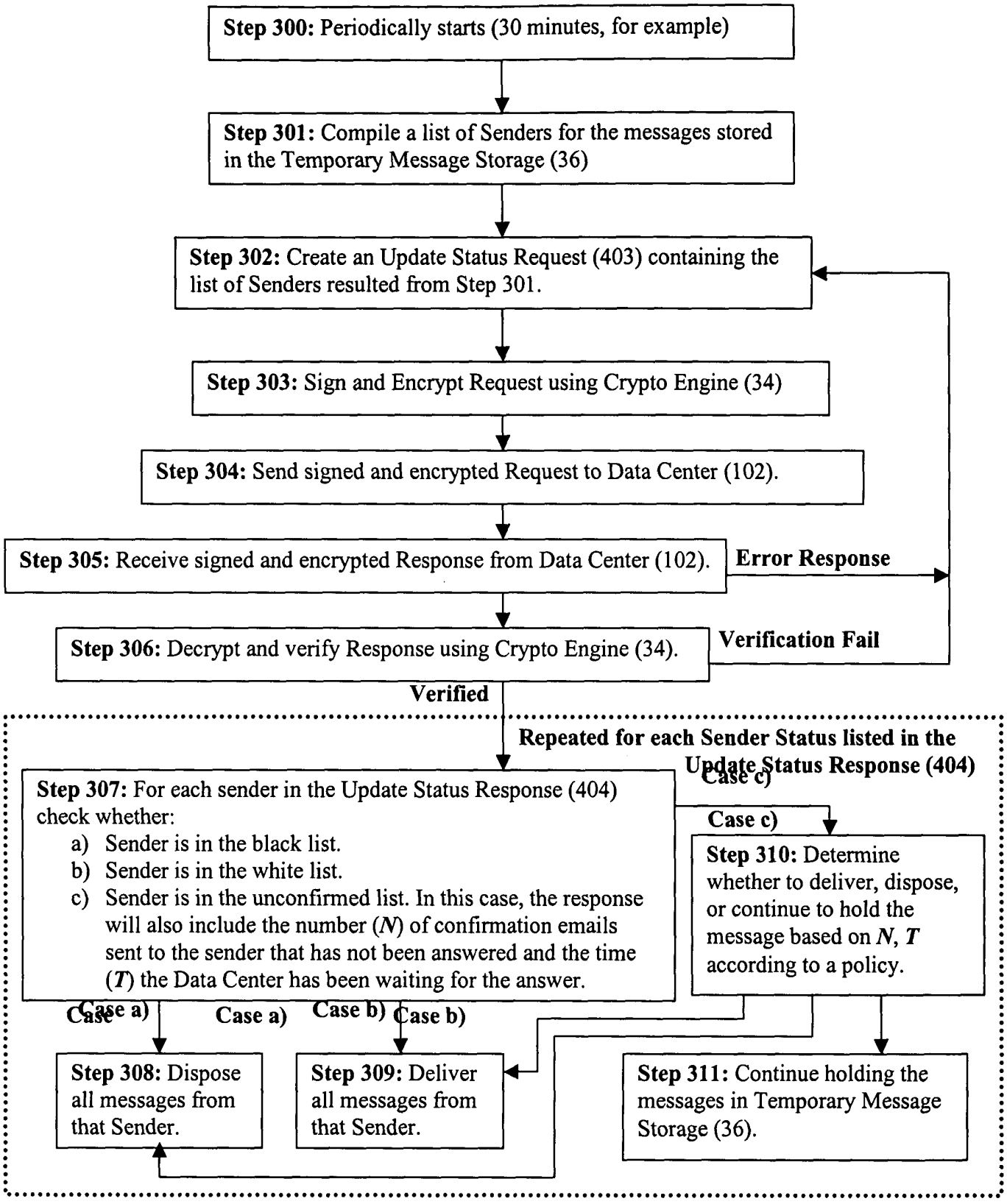
Step 300: Periodically starts (30 minutes, for example)
Step 301: Compile a list of Senders for the messages stored in the Temporary Message Storage (36)
Step 302: Create an Update Status Request (403) containing the list of Senders resulted from Step 301.
Step 303: Sign and Encrypt Request using Crypto Engine (34)
Step 304: Send signed and encrypted Request to Data Center (102).
Step 305: Receive signed and encrypted Response from Data Center (102).
Error Response
Step 306: Decrypt and verify Response using Crypto Engine (34).
Verification Fail
Verified
Repeated for each Sender Status listed in the Update Status Response (404)
Step 307: For each sender in the Update Status Response (404) check whether:
a) Sender is in the black list.
b) Sender is in the white list.
c) Sender is in the unconfirmed list. In this case, the response will also include the number (N) of confirmation emails sent to the sender that has not been answered and the time (T) the Data Center has been waiting for the answer.
Case a)
Case b)
Case c)
Step 308: Dispose all messages from that Sender.
Step 309: Deliver all messages from that Sender.
Step 310: Determine whether to deliver, dispose, or continue to hold the message based on N, T according to a policy.
Step 311: Continue holding the messages in Temporary Message Storage (36).

Figure 3

Spam Filter Sends:

Check Sender Request (401)

SPAM Filter Type
Sender Email Address
Subject
Time
Number of Recipients
List of Recipients (Each item includes Recipient's email address and recipient type, such as To, Cc, or Bcc.)
Random Number

Data Center Returns:

Sender Status Response (402)

Sender Email Address
Sender Status (in white list, in black list, or in unconfirmed list)
Number (*N*) of unanswered confirmation emails. (Present only when Sender is in the unconfirmed list)
The maximum time (*T*) the data center has been waiting for the answer to the confirmation emails. (Present only when Sender is in the unconfirmed list)
Pass code (present when pass code is required for the white list sender).
Random Number

Spam Filter Sends:

Update Status Request (403)

SPAM Filter Type
Number of Senders
List of Senders
Random Number

Data Center Returns:

Update Status Response (404)

Number of Senders
List of Sender Status. Each item contains the same data items in **Sender Status Response (402)** except the Random Number.
Random Number

Figure 4

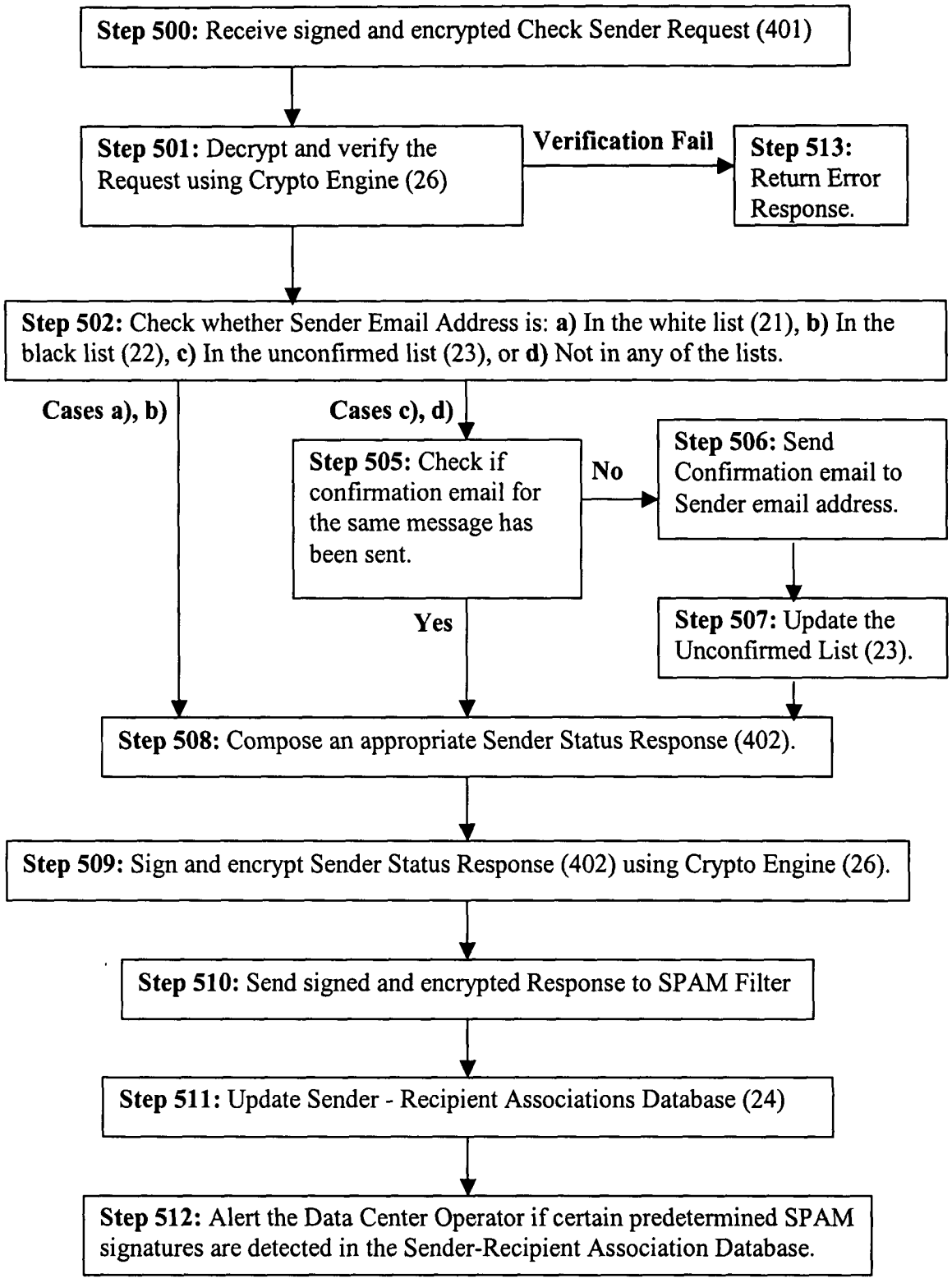
Step 500: Receive signed and encrypted Check Sender Request (401)
Step 501: Decrypt and verify the Request using Crypto Engine (26)
Verification Fail
Step 513: Return Error Response.
Step 502: Check whether Sender Email Address is: a) In the white list (21), b) In the black list (22), c) In the unconfirmed list (23), or d) Not in any of the lists.
Cases a), b)
Cases c), d)
Step 505: Check if confirmation email for the same message has been sent.
No
Step 506: Send Confirmation email to Sender email address.
Yes
Step 507: Update the Unconfirmed List (23).
Step 508: Compose an appropriate Sender Status Response (402).
Step 509: Sign and encrypt Sender Status Response (402) using Crypto Engine (26).
Step 510: Send signed and encrypted Response to SPAM Filter
Step 511: Update Sender - Recipient Associations Database (24)
Step 512: Alert the Data Center Operator if certain predetermined SPAM signatures are detected in the Sender-Recipient Association Database.

Figure 5

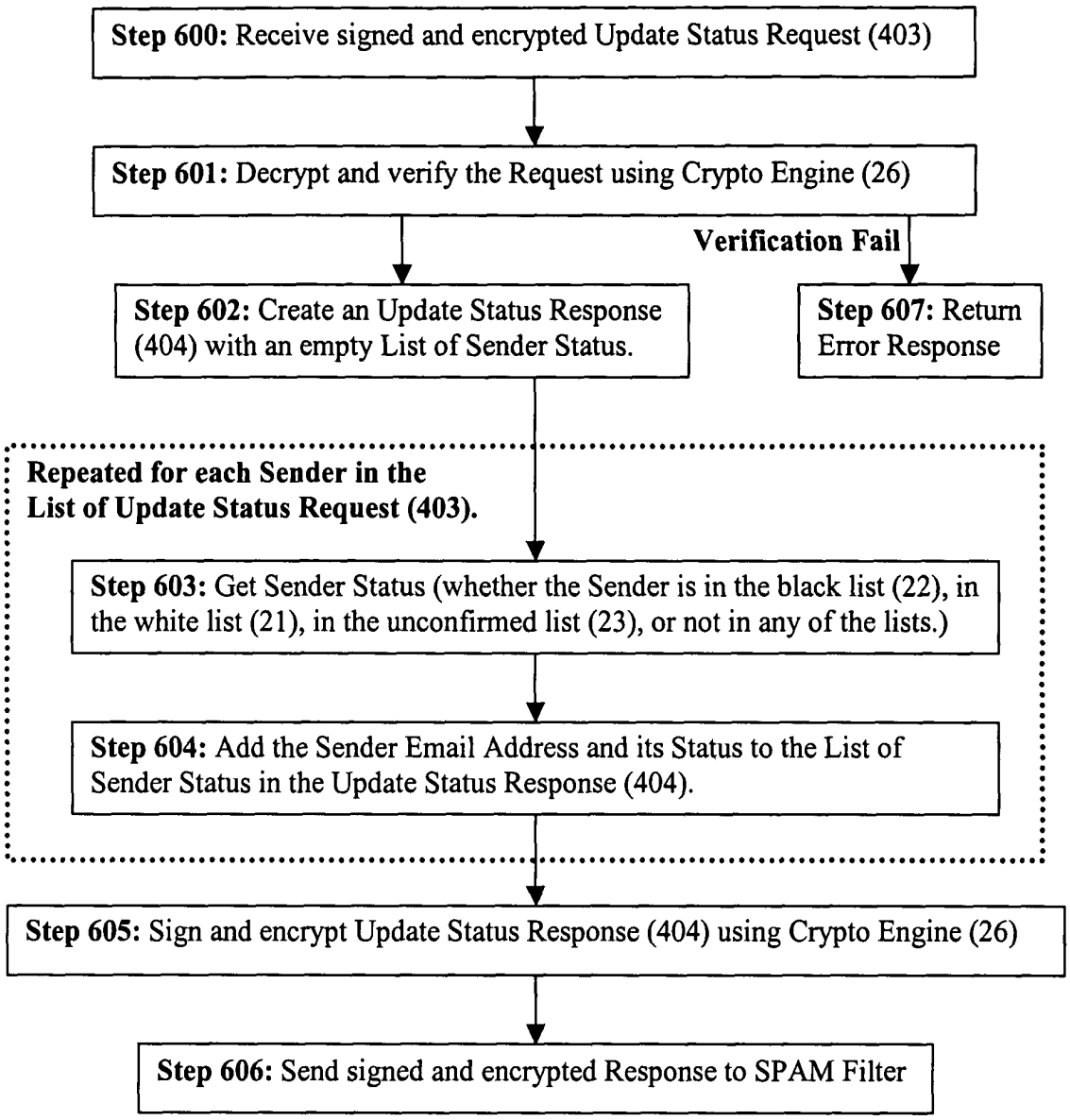
Step 600: Receive signed and encrypted Update Status Request (403)
Step 601: Decrypt and verify the Request using Crypto Engine (26)
Verification Fail
Step 602: Create an Update Status Response (404) with an empty List of Sender Status.
Step 607: Return Error Response
Repeated for each Sender in the List of Update Status Request (403).
Step 603: Get Sender Status (whether the Sender is in the black list (22), in the white list (21), in the unconfirmed list (23), or not in any of the lists.)
Step 604: Add the Sender Email Address and its Status to the List of Sender Status in the Update Status Response (404).
Step 605: Sign and encrypt Update Status Response (404) using Crypto Engine (26)
Step 606: Send signed and encrypted Response to SPAM Filter

Figure 6

From: antispamcenter@zixcorp.com
Sent: Friday, April 25, 2003 10:39 AM
To: john@example.com
Subject: Re: Conference call schedule

Your email message titled "Conference call schedule" sent at Friday, April 25, 2003 10:25 AM has been held temporarily and will not be delivered to those recipients who use Zix SPAM filter. The reason is because you are not currently in the trusted sender database. To be added to the database, click the following hyperlink and enter the authorization code below. Your original message will be delivered and you will be added to the trusted sender database. After that, you will not receive any more notices like this one and your future messages will be immediately delivered to all recipients.
http://antispam.zixcorp.com/antispam.cgi?id=8afc2389cb98d401

Authorization Code:

Figure 7

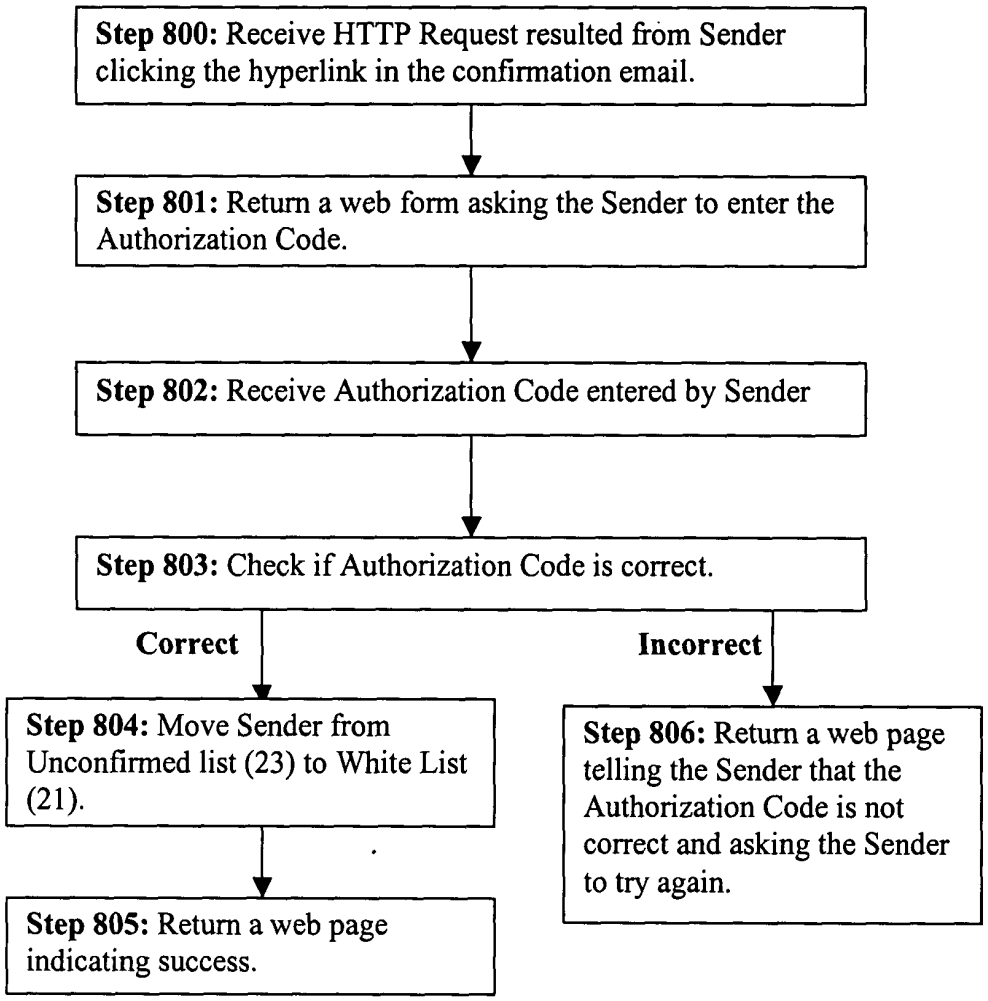

Figure 8 (Sender Response Processor)

Email notice sent when the pass code requirement is turned on

From: antispamcenter@zixcorp.com
Sent: Friday, April 25, 2003 10:39 AM
To: john@example.com
Subject: Pass code required

According to user complaints and the data we collected, a large number of unsolicited email messages appear to be sent from your email address john@example.com. It is possible that a spammer is sending out spams pretending to be from your email address. In order to filter out spams while letting your messages to go through, you need to include the following pass code on the first line of every email message you send out. The pass code will allow your messages to pass through the Zix SPAM filters while blocking spammer's messages pretending to be from you. Please note, a message sent without the correct pass code will be blocked by the Zix SPAM filters.

370urebn3s983sg

From the following site, you may download plug-ins that will automatically insert the pass code into every message you send out. The plug-in will put the pass code in a header of the email message, instead of on the first line, so that it will not be seen by the recipient.

http://www.zixcorp.com/antispam/download.html

Email notice sent when the pass code requirement is turned off

From: antispamcenter@zixcorp.com
Sent: Friday, April 25, 2003 10:39 AM
To: john@example.com
Subject: Pass code not required any more

We are pleased to inform you that the spammer who has been sending spams pretending to be from your emails address has been tracked down and his ISP has terminated his account. He is not sending any more spams pretending to be from your email address. As a result, we have turned off the pass code requirement on your email address. You do not have to include the pass code in your email messages any more.

Figure 9